UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/099,779	03/14/2002	Todd Weston Arnold	AUS920010984US1	4841

40412 7590 03/03/2006

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/099,779	ARNOLD ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6-8,13,14 and 19-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,6-8,13,14 and 19-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 12/11/2005.

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 6 – 8, 13, 14, and 19 – 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the added limitation "the second key" in line 26. There is insufficient antecedent basis for this limitation in the claim. For the purpose of examination the examiner will presume the applicant to mean “the second password”.

Similar to claim 1, claims 8 and 14 each recites the added limitation "the second key" within. There is insufficient antecedent basis for this limitation in these claims. For

the purpose of examination the examiner will presume the applicant to mean "the second password".

Claim 13 depends upon the canceled claim 12. There is insufficient antecedent basis for claim 13.

All other depending claims have been rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6, 7, 8, 14, 19, 20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Al-Salqan, "Method and Apparatus for Encoding Keys", U.S. Patent, 6,549,626 in view of Hosokawa, "Internet Broadcast Billing System", U.S. Patent Publication, 2001/0023416 A1.

Regarding claim 1, Al-Salqan discloses:

receiving, at a security module, a first password corresponding a software application (Al-Salqan, col. 2, lines 12-28, 49-63; fig. 2, elem. 204); *generating, at a security module, a first mask value based on the first password* (Al-Salqan, col. 4, lines 29-46; fig. 2); *combining, at a security module, the first mask value with a first encryption key* (Al-Salqan, col. 4, lines 49-52; fig. 2);

encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key (Al-Salqan, fig. 2). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).

returning the encrypted tied key to the software application (Al-Salqan, fig. 2, elem. 246). Al-Salqan discloses the returning of the encrypted tied key to what is termed the "user". Clear to those of ordinary skill in the art, the term "user" is a reference to a user employing a computer-implemented application, an interface to the security module. For understanding of such, the applicant's representative is respectfully invited to consider the Applicant's own disclosure of the prior art, which evidences that which was clear to those having knowledge of technology (Spec. pg. 1, lines 16-17, 22-24; pg. 2, line 27 – pg. 3, line 2). Herein, the Applicants clearly equate, viewing as interchangeable, a customer (a "human") with an application, meaning, more specifically, that a human does not interact with the computer system as he/she would interact with another human, but instead, interacts with the computer system via an application. Thus, when one of ordinary skill in the art refers to a "customer" as using

an encryption key within a computer system, in actuality, that one is appropriately and reasonably referring to an "application" in employment by a user. Al-Salqan discloses a computer software security module as outputting an electronic key to a "user" via an output (fig. 2, elem. 246). Truly, one of ordinary skill in the art would believe as absurd the thought that Al-Salqan was actually implying a direct interaction between the software and human, such as the dropping of digital data bits into the palm of a the user's hand. No indeed, Al-Salqan is merely describing technology in harmony with the understanding of those having technical knowledge, and in a manner similar to the applicant's themselves. In accordance, Al-Salqan discloses a complete computer system comprising hardware and software for implementing both a security module and software means for a user to interact with and employ the security module (Al-Salqan, col. 3, lines 16-52).

determining, at the software application, that the encrypted tied key corresponds to the security module; in response to the determining, sending the encrypted tied key and a second password form the software application to the security module over a computer network, the second password being the same as the first password (Al-Salqan, fig. 3, elems. 302,306). Herein, Al-Salqan discloses the transmission of a encrypted tied key and password within an interconnected group of computing elements. The examiner would like to point out that the limitation *determining, at the software application,* claimed within a method comprising steps, does not indicate who or what does the determining and how such a determination is conducted. Furthermore, the examiner takes note that the claim vaguely claims a correspondence

between a key and module, but provides no indication of what comprises the correspondence. Al-Salqan discloses the above limitations, as the correct password and a corresponding tied key of a user is passed to the security module via the software means for enabling such interaction between the user and security module (Al-Salqan, col. 3, lines 16-52).

receiving, at the security module, the encrypted tied key and the second password from the software application; in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second key, the combining resulting in a recovered tied key (Al-Salqan, fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).

generating a second mask value based on the second password (Al-Salqan, col. 4, lines 29-46; fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05);

separating a recovered encryption key from the recovered tied key using the second mask value (Al-Salqan, col. 7, lines 45-49; fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teaching of the recovery of an recovered encryption key from the recovered tied key ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).

and encrypting data provided by the software application using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 1, lines 21-28; col. 7, lines 48,49; col. 3, lines 52-56). First, regarding the limitation "provided by the software application", the examiner notes that such is descriptive language describing data. This has added no further structure to the claim, the data itself being non-functional descriptive material. Additionally, the examiner points out that the above-mentioned limitation provides no indication as to how the software provides data to be encrypted or to what or whom the software provides the data to be encrypted. Al-Salqan discloses the encryption of symmetric encryption keys. Al-Salqan discloses that keys, when they are requested and obtained by the user, are used to encrypt data (Al-Salqan, col. 3, lines 55-57; col. 7, lines 48-49). When an encryption key becomes lost, an authorized user of the key may recover the key for use again (Al-Salqan, col. 1, lines 61-65) Al-Salqan discloses that such symmetric encryption keys are used to encrypt and decrypt data, and for such, an application of software is used (Al-Salqan, col. 1, lines 61-65; col. 3, lines 16-52).

Al-Salqan discloses a system designed to ensure the secrecy of a data encryption key, such as a symmetric key. Secrecy is accomplished by encrypting the data encryption key. However, though Al-Salqan discloses enabling the secrecy of a symmetric data encryption key, it does not disclose the enabling of the authenticity of the key. Thus, Al-Salqan does not disclose wherein the first "encryption key" *is derived from a generated key and a known value the combining resulting a tied key* or that the

recovered "encryption key" includes *a recovered generated key and a recovered known value*.

Hosokawa discloses a method for the verification of the authenticity of a data-encryption key, the method being performed "as a security measure" (Hosokawa, par 37). This "security measure" of ensuring authenticity is additional to the security measure of ensuring secrecy - encrypting the data encryption key. The method comprises the creation of a "tied key", or an "encryption key" derived from a generated key and a known value (Hosokawa, par. 32, lines 8-12; par. 33, lines 1-5; par. 37, lines 11-13; par. 44, lines 11-18). Hosokawa attaches a "known value", a digital signature, to generated key, and thereby creates a "tied key". After the "tied key" is decrypted, the attached digital signature is compared to an authentic digital signature so as to verify the authenticity of the generated key. If authentic, the generated key is used for encrypting data. Thus, Hosokawa discloses a method usable to verify the authenticity of an encryption key, the method ensuring a measure of security.

It would have been obvious to one of ordinary skill in the art to combine the method of Hosokawa with the system of Al-Salqan. This would have been obvious because one of ordinary skill in the art would have been motivated to enhance the security of the system of Al-Salqan, by not only enabling the secrecy of the data encryption key, but also the authentication of the data encryption key. Thus, a more secure system is provided.

Regarding claim 6, the combination of Al-Salqan and Hosokawa disclose:

determining whether the recovered known value is correct; and processing a data file based on the determination (Hosokawa, col. 2, pars. 32, 33; Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claim 7, the combination of Al-Salqan and Hosokawa disclose:

wherein the processing is selected from the group consisting of encrypting the data file using the recovered generated key and decrypting the data file using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claim 22, the combination of Al-Salqan and Hosokawa disclose:

wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted (Hosokawa, par. 41). The combination of Al-Salqan and Hosokawa disclose that the key is appropriately used for securing data, thus the key is at a level of security suitable for securing sensitive data.

Regarding claims 8, 14, 19, and 20, they are the system means and computer program product claims implementing the method of claims 1, 6, and 7, and they are rejected, at least, for the same reasons. Further, regarding claim 8 specifically, it is rejected because the combination of Al-Salqan and Hosokawa disclose:

one or more processors; a memory accessible by the processors; one or more nonvolatile storage devices accessible by the processors; a hardware security module

accessible by the processors; a data security tool for securing data using the hardware security module (Al-Salqan, figs. 1, 2; col. 3, lines 16-45).

Claims 21, 23, 24, 26, 27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Al-Salqan and Hosokawa in view of the Applicant's Admitted Prior Art.

Regarding claims 21 and 23, the combination of Al-Salqan and Hosokawa does not disclose *wherein the security module is a separate hardware security module* and *wherein encrypting the data is performed within the security module*. However, it would have been logical to one of ordinary skill in the art employ a *security* module to provide *security* to data. Furthermore, it would have been logical to one of ordinary skill in the art to utilize hardware versus software, as hardware is known to provide advantages in security and performance. The applicants, themselves, attest to the above facts in their disclosure of the known prior art. The applicants have admitted that prior art comprises the use of hardware security modules and that the hardware security modules are useable for encrypting data that a user desires to be secured (Spec., page 2, pars. 1 – 3).

It would have been obvious to one of ordinary skill in the art to employ the prior art teachings disclosed by the Applicants within the combination of Al-Salqan and Hosokawa. This would have been obvious because one of ordinary skill in the art would

have been motivated to employ methods that are logical and have been known to be feasible in prior art technology.

Regarding claims 24, 26, 27, and 29, they are the system means and computer program product claims implementing the method of claims 21 and 23, and they are rejected, at least, for the same reasons.

Response to Arguments

Applicant's arguments filed 12/11/05 have been fully considered but they are not persuasive.

The applicant's representative argues primarily that:

I. *As discussed with the Examiner, Applicants have amended the independent claims to include the limitations of original claims 2 – 5* (Remarks, pg. 4, par. 4).

The examiner would like to respectfully point out that the applicant's representative is mistaken. While the added limitations to the amended claims 1, 8, and 14 bear a semblance to the limitations found within the original claims of 2 – 5, a comparison of the newly added limitations to the original limitations reveals that the newly added limitations are not the same limitations found within the original claims.

Thus, the newly added limitations to the independent claims 1, 8, and 14 comprise limitations that have not been previously considered in the prior office action.

II. *First, Applicants claim "receiving, at security module, a first password corresponding to a software application." Al-Salqan's passwords do not correspond to a software application* (Remarks, pg. 6, par. 2).

In response, the examiner asserts that Al-Salqan teaches software employed by user to provision a password and a password that has been provisioned by software (refer to the discussion respecting the rejection of claim 1). Naturally, a correspondence exists between a provisioned password and password provisioning software simply by virtue of the provisioning. The examiner respectfully points out that if the applicant's representative desires to argue a more specific type of correspondence, then such a particular type of correspondence should be claimed - as opposed to nebulously claiming "corresponding".

III. *Second, Applicant's claim "returning the encrypted tied key to the software application"...*

As can be seen from the above excerpt, Al-Salqan teaches passing the encrypted key to a storage area or to a user for storage elsewhere. As such, Al-Salqan never teaches or suggests a software application ... (Remarks, pg. 7).

In response the examiner respectfully asserts that the applicant's representative is mistaken and has mischaracterized the prior art. The examiner affirms, as is

explained in the rejection of claims 1, 8, and 14, that Al-Salqan discloses software for implementing a security module as well as software for enabling a user (human) to interact with the security module. Such an interface exists, as a human does not interact with a software security module directly. Naturally the inputs and outputs of the security module (Al-Salqan, figs. 2, 3) do not connect directly to a human (i.e. electronic data bits dropped into the palm of a user's hand). The examiner finds the argument of the applicant's representative (namely, there does not exist an application of software between a user and the security module) to be unpersuasive.

Furthermore, it is interesting to note, that the applicant's themselves, similar to Al-Salqan, interchangeably use terms referring to humans when describing the interaction between an application of software and a security module (Spec., pg. 2, par. 4). Thus, the examiner finds the arguments of the applicant's representative to be inconsistent with the applicant's disclosure.

IV. *Third, Applicants claim "encrypting data provided by the software application using the recovered generated key." Since Applicants' claim 1 should be viewed as a whole, the software application provides passwords, receives the encrypted tied key, and provides data to be encrypted by the security module. Al-Salqan never teaches or suggests a software application performing these limitations while interacting with the security module as claimed by Applicants* (Remarks, pg. 8, par. 1).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies

(i.e., *the software application provides passwords, receives the encrypted tied key, and provides data to be encrypted by the security module*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
AU: 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER